REMARKS

Claims 1-50 and 83-93 were examined and reported in the Office Action. Claims 1-50 and 83-93 are rejected. Claim 3 is canceled. Claims 1-2, 4-50 and 83-93 are amended. Claims 1-2 and 4-93 remain.

Applicant requests reconsideration of the application in view of the following remarks.

I.   35 U.S.C. §112, second paragraph

It is asserted in the Office Action that claims 1-20 and 83-93 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant has amended claims 1 and 2-20 and 83-93 to overcome the 35 U.S.C. §112, second paragraph rejection. In particular, Applicant has amended the limitation of "use device" to "device."

Accordingly, withdrawal of the 35 U.S.C. §112, second paragraph rejection for claims 1-20 and 83-93 is respectfully requested.

II.   35 U.S.C. § 102(e)

A.   It is asserted in the Office Action that claims 37-39 and 44-46 are rejected under 35 U.S.C. § 102(e), as being anticipated by U. S. Patent No. 6,980,672 issued to Saito et al ("Saito"). Applicant respectfully traverses the aforementioned rejection for the following reasons.

According to MPEP §2131,

> '[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.' (Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). 'The identical invention must be shown in as complete detail as is contained in the ... claim.' (Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)). The elements must be arranged as required by the claim, but this is

not an ipsissimis verbis test, *i.e.*, identity of terminology is not required. (In re Bond, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990)).

Applicant's amended claim 37 contains the limitations of

> [a] biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising: drive means for locking/unlocking the door; storage means for storing the biometrical information of the user; and processing means for controlling said drive means to unlock the door on the basis of matching between stored information in said storage means and detected information from a sensor for detecting the biometrical information of the user, said processing means controls said drive means to unlock the door on the basis of matching between the stored information in said storage means and the fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information wherein the fingerprint authentication token is independent of the main body and physically separated from the main body.

Applicant's amended claim 44 contains the limitations of

> [a] lock/unlock method for a biometrical information authentication storage which locks or unlocks a door of a main body in storing an article in the main body or taking out the article stored in the main body, and also unlocks the door on the basis of authentication of biometrical information of a user, comprising: the first step of unlocking the door on the basis of matching between stored information stored in storage means in advance and detected information from a sensor for detecting the biometrical information of the user; and processing the first step comprises a second step of unlocking the door on the basis of matching between the stored information in the storage means and a fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, wherein the token is independent of the main body and physically separated from the main body.

Saito discloses a lock with a pressure-based fingerprint sensor where the sensor detects the fingerprint pattern of the finger that presses the sensor. A matching circuit prepares a fingerprint code based on the detected fingerprint pattern and the code is compared with registered fingerprint codes stored in a memory device to determine whether there is a match. If there is a match, a control unit unlocks the locking mechanism. Saito, however, does not teach, disclose or suggest

> processing means for controlling said drive means to unlock the door on the basis of matching between stored information in said storage means and detected information from a sensor for detecting the biometrical information of the user, said processing means controls said drive means to unlock the door on the basis of matching between the stored information in said storage means and the fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information <u>wherein the fingerprint authentication token is independent of the main body and physically separated from the main body,</u>

nor

> a second step of unlocking the door on the basis of matching between the stored information in the storage means and a fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, wherein the token is independent of the main body and physically separated from the main body.

Further, Saito does not teach, disclose or suggest the limitations in claims 39 and 46 of

> <u>each time the door is locked the fingerprint image received from the authentication token is stored in the storage means,</u> and unlock means for controlling said drive means to unlock the door when the fingerprint image of the user, which is transmitted from the fingerprint authentication token, is received in taking out the article stored in the main body, and the received fingerprint image <u>transmitted from the fingerprint authentication token, and</u> matches the <u>fingerprint image stored</u> in said storage means.

Therefore, since Saito does not disclose, teach or suggest all of Applicant's amended claims 37 and 44 limitations, Applicant respectfully asserts that a *prima facie* rejection under 35 U.S.C. § 102(e) has not been adequately set forth relative to Saito. Thus, Applicant's amended

claims 37 and 44 are not anticipated by Saito. Additionally, the claims that directly or indirectly depend on claims 37 and 44, namely claims 38-39, and 45-46, respectively, are also not anticipated by Saito for the same reason.

Accordingly, withdrawal of the 35 U.S.C. §102(e) rejection for claims 37-39 and 44-46 is respectfully requested.

B. It is asserted in the Office Action that claims 1-6, 8, 83-86 are rejected under 35 U.S.C. § 102(e), as being anticipated by U. S. Patent No. 6,484,260 issued to Scott et al ("Scott"). Applicant respectfully traverses the aforementioned rejection for the following reasons.

Applicant's amended claim 1 contains the limitations of

> a personal collation unit including a sensor for detecting the biometrical information of the user and outputting a detection result as sensing data, a storage unit which stores in advance registered data to be collated with the biometrical information of the user, and a collation unit for collating the registered data stored in said storage unit with the sensing data from said sensor and outputting a collation result as authentication data representing a user authentication result; a communication unit for transmitting the authentication data from said personal collation unit to the device as communication data, and a protocol conversion unit for converting data format of the communication data from said communication unit into a predetermined data format and transmitting the communication data to the device, wherein said personal collation unit and communication unit are integrated.

Scott discloses a personal identification system using a biometric sensor to allow access to a secure facility. Scott further discloses an encoder has an encryption algorithm that uses a private key and a memory can store an ID code. Scott, however, does not teach, disclose or suggest conversion of the data format, which is different from encrypting data. That is, Scott does not teach, disclose or suggest "a protocol conversion unit for converting data format of the communication data from said communication unit into a predetermined data format and transmitting the communication data to the device."

Regarding Applicant's amended claim 83, Scott does not teach, disclose or suggest "the dynamic information changes each time it is generated."

Regarding Applicant's amended claim 84, in Applicant's claimed invention the authentication data is transmitted to the device not only when the authentication is successful, but also when the authentication fails. As a result, even if a user failed to be authenticated, various assistances may be given to the user. For example, a device could provide a user with help information so that the user could know what to do if he or she fails the authentication, and also a device could detect irregular use of a device, such as a token. Scott, however, does not teach, disclose or suggest "when the collation result indicates that the authentication is successful, outputting the authentication data to said encryption circuit, and when the collation result indicates that the authentication fails, outputting the authentication data to said first communication circuit."

In Applicant's claim 85, the number of digits of the information transmitted is changed when the authentication fails. Therefore, the result of the authentication can be recognized by checking the number of the digits, without decoding the encrypted information, so that informs the right user of potential dishonest use, and/or countermeasures against dishonest use can be taken. Scott, however, does not teach, disclose or suggest "when the collation result indicates that the authentication is successful, instructing said encryption circuit to generate the encrypted data, and when the collation result indicates that the authentication fails, outputting data whose number of digits is different from that of the encrypted data that would be produced if the authentication was successful to said first communication circuit."

Therefore, since Scott does not disclose, teach or suggest all of Applicant's amended claim 1 limitations, Applicant respectfully asserts that a *prima facie* rejection under 35 U.S.C. § 102(e) has not been adequately set forth relative to Scott. Thus, Applicant's amended claim 1 is not anticipated by Scott. Additionally, the claims that directly or indirectly depend on claim 1, namely claims 2, 4-6, 8 and 83-86, are also not anticipated by Scott for the same reason.

Accordingly, withdrawal of the 35 U.S.C. §102(e) rejection for claims 1-6, 8, 83-86 is respectfully requested.

III.   35 U.S.C. § 103(a)

A.   It is asserted in the Office Action that claims 9-18, 20-36, and 87-93 are rejected under 35 U.S.C. § 103(a), as being unpatentable over Scott in further view of U. S. Patent No. 6,957,338 issued to Sumino ("Sumino"). Applicant respectfully traverses the aforementioned rejection for the following reasons.

According to MPEP §2142

> "[t]o establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure." (In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

Further, according to MPEP §2143.03, "[t]o establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. (In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974)." "*All words in a claim must be considered in judging the patentability of that claim against the prior art.*" (In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970), emphasis added.)

Applicant's claim 1 contains the limitations of "a protocol conversion unit for converting data format of the communication data from said communication unit into a predetermined data format and transmitting the communication data to the device."

Applicant's claim 10 contains the limitations of "an authentication token which is normally held by the user and, when the user is to use said device, the authentication token

connected to said device and to perform user authentication on the basis of the biometrical information of the user."

Applicant's claim 21 contains the limitations of "an authentication token which is normally held by the user and, when the user is to use said service providing apparatus, connected to said service providing apparatus to perform user authentication on the basis of the biometrical information of the user."

Applicant's claim 25 contains the limitations of

> the authentication token stores in advance a password of the authentication token and token identification information for identifying the authentication token, performs collation on the basis of the biometrical information detected from the user to check whether the user is an authentic user, and when a collation result indicates that collation is successful, transmits the password and token identification information to the service providing apparatus as communication data, and the service providing apparatus stores the token identification information and password of the authentication token in advance in a first database in association with each other, collates the password contained in the communication data received from the authentication token with a password obtained from the first database using the token identification information as a key, and provides the service to the user on the basis of a collation result.

Applicant's claim 29 contains the limitations of

> in the service providing apparatus, storing token identification information and a password of the authentication token in a first database in advance in association with each other; in the authentication token, after collation of the user based on the biometrical information detected from the user, and when a collation result indicates that collation is successful, receiving communication data containing the password of the authentication token and the token identification information for identifying the authentication token, which is transmitted for the authentication token.

Applicant's claim 33 contains the limitations of

> in the service providing apparatus, store token identification information and a password of the authentication token in a first database in advance in association with each other; in the authentication token, after collation of the user based on the biometrical information detected from the user, and when a collation result indicates that collation is successful, receive communication data containing the password of the authentication token and the token identification information for identifying the authentication token, which is transmitted for the authentication token.

Scott discloses a personal identification system using a biometric sensor to allow access to a secure facility. Scott further discloses an encoder has an encryption algorithm that uses a private key and a memory can store an ID code.

Sumino discloses an individual authentication system using an authentication card for storing biological information and a password for identifying a registered user.

Sumino and Scott, however, do not teach, disclose or suggest Applicant's: claim 1 limitations of "a protocol conversion unit for converting data format of the communication data from said communication unit into a predetermined data format and transmitting the communication data to the device," claim 10 limitations of "an authentication token which is normally held by the user and, when the user is to use said device, the authentication token connected to said device and to perform user authentication on the basis of the biometrical information of the user," claim 21 limitations of "an authentication token which is normally held by the user and, when the user is to use said service providing apparatus, connected to said service providing apparatus to perform user authentication on the basis of the biometrical information of the user," claim 25 limitations of

> the authentication token stores in advance a password of the authentication token and token identification information for identifying the authentication token, performs collation on the basis of the biometrical information detected from the user to check whether the user is an authentic user, and when a collation result indicates that collation is successful, transmits the password and token identification information to the service providing apparatus as communication data, and the service providing apparatus stores

the token identification information and password of the
authentication token in advance in a first database in association
with each other, collates the password contained in the
communication data received from the authentication token with a
password obtained from the first database using the token
identification information as a key, and provides the service to the
user on the basis of a collation result,

claim 29 limitations of

in the service providing apparatus, storing token identification
information and a password of the authentication token in a first
database in advance in association with each other; in the
authentication token, after collation of the user based on the
biometrical information detected from the user, and when a
collation result indicates that collation is successful, receiving
communication data containing the password of the authentication
token and the token identification information for identifying the
authentication token, which is transmitted for the authentication
token,

nor claim 33 limitations of

in the service providing apparatus, store token identification
information and a password of the authentication token in a first
database in advance in association with each other; in the
authentication token, after collation of the user based on the
biometrical information detected from the user, and when a
collation result indicates that collation is successful, receive
communication data containing the password of the authentication
token and the token identification information for identifying the
authentication token, which is transmitted for the authentication
token.

Neither Scott, Sumino, and therefore, nor the combination of the two, teach, disclose or

suggest all of Applicant's claims 1, 10, 21, 25, 29 and 33 limitations, as listed above. Since

neither Scott, Sumino, and therefore, nor the combination of the two do not teach, disclose or

suggest all the limitations of Applicant's claims 1, 10, 21, 25, 29 and 33, Applicant's claims 1,

10, 21, 25, 29 and 33 are not obvious over Scott in view of Sumino since a *prima facie* case of

obviousness has not been met under MPEP §2142. Additionally, the claims that directly or

indirectly depend from claims 1, 10, 21, 25, 29 and 33, namely claims 9, 11-18, 20 and 87-93,

22-24, 26-28, 30-32, and 34-36, respectively, would also not be obvious over Scott in view of Sumino for the same reason.

Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejections for 9-18, 20-36, and 87-93 are respectfully requested.

B.   It is asserted in the Office Action that claims 40, 41, 43, 47, 48 and 50 are rejected under 35 U.S.C. § 103(a), as being unpatentable over Saito in further view of Scott. Applicant respectfully traverses the aforementioned rejection for the following reasons.

Applicant's claims 40, 41 and 43 either directly or indirectly depend on claim 37. Claims 47, 48 and 50 either directly or indirectly depend on claim 44.

Applicant's claim 37 contains the limitations of

> said processing means controls said drive means to unlock the door on the basis of matching between the stored information in said storage means and the fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, wherein the fingerprint authentication token is independent of the main body and physically separated from the main body.

Applicant's claim 44 contains the limitations of

> processing the first step comprises a second step of unlocking the door on the basis of matching between the stored information in the storage means and a fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, wherein the token is independent of the main body and physically separated from the main body.

Saito discloses a lock with a pressure-based fingerprint sensor where the sensor detects the fingerprint pattern of the finger that presses the sensor. A matching circuit prepares a fingerprint code based on the detected fingerprint pattern and the code is compared with registered fingerprint codes stored in a memory device to determine whether there is a match. If there is a match, a control unit unlocks the locking mechanism.

Scott discloses a personal identification system using a biometric sensor to allow access to a secure facility. Scott further discloses an encoder has an encryption algorithm that uses a private key and a memory can store an ID code.

Saito and Scott, however, do not teach, disclose or suggest Applicant's: claim 37 limitations of

> said processing means controls said drive means to unlock the door on the basis of matching between the stored information in said storage means and the fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, wherein the fingerprint authentication token is independent of the main body and physically separated from the main body,

nor Applicant's claim 44 limitations of

> processing the first step comprises a second step of unlocking the door on the basis of matching between the stored information in the storage means and a fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, wherein the token is independent of the main body and physically separated from the main body.

Since neither Saito, Scott, and therefore, nor the combination of the two do not teach, disclose or suggest all the limitations of Applicant's claims 37 and 44, Applicant's claims 37 and 44 are not obvious over Saito in view of Scott since a *prima facie* case of obviousness has not been met under MPEP §2142. Additionally, the claims that directly or indirectly depend from claims 37 and 44, namely claims 40, 41 and 43, and 47, 48 and 50, respectively, would also not be obvious over Saito in view of Scott for the same reason.

Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejections for claims 40, 41, 43, 47, 48 and 50 respectfully requested.

C.   It is asserted in the Office Action that claims 7 and 19 are rejected under 35 U.S.C. § 103(a), as being unpatentable over Scott in view of Sumino and further in view of Scott. Applicant respectfully traverses the aforementioned rejection for the following reasons.

Applicant's claim 7 indirectly depends on claim 1. Claim 19 indirectly depends on claim 10.

Scott discloses a personal identification system using a biometric sensor to allow access to a secure facility. Scott further discloses an encoder has an encryption algorithm that uses a private key and a memory can store an ID code. Scott, however, does not teach, disclose or suggest conversion of the data format, which is different from encrypting data.

Sumino discloses an individual authentication system using an authentication card for storing biological information and a password for identifying a registered user.

Sumino and Scott, however, do not teach, disclose or suggest Applicant's: claim 1 limitations of "a protocol conversion unit for converting data format of the communication data from said communication unit into a predetermined data format and transmitting the communication data to the device," nor claim 10 limitations of "an authentication token which is normally held by the user and, when the user is to use said device, the authentication token connected to said device and to perform user authentication on the basis of the biometrical information of the user."

Since neither Sumino, Scott, and therefore, nor the combination of the two do not teach, disclose or suggest all the limitations of Applicant's claims 1 and 10, Applicant's claims 1 and 10 are not obvious over Sumino in view of Scott in view of Sumino since a *prima facie* case of obviousness has not been met under MPEP §2142. Additionally, the claims that directly or indirectly depend from claims 1 and 10, namely claims 7, and 19, respectively, would also not be obvious over Sumino in view of Scott in view of Sumino for the same reason.

Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejection for claims 7 and 19 is respectfully requested.

D.   It is asserted in the Office Action that claims 42 and 49 are rejected under 35 U.S.C. § 103(a), as being unpatentable over Saito in view of Scott and further in view of Saito. Applicant respectfully traverses the aforementioned rejection for the following reasons.

Saito discloses a lock with a pressure-based fingerprint sensor where the sensor detects the fingerprint pattern of the finger that presses the sensor. A matching circuit prepares a fingerprint code based on the detected fingerprint pattern and the code is compared with registered fingerprint codes stored in a memory device to determine whether there is a match. If there is a match, a control unit unlocks the locking mechanism.

Scott discloses a personal identification system using a biometric sensor to allow access to a secure facility. Scott further discloses an encoder has an encryption algorithm that uses a private key and a memory can store an ID code. Scott, however, does not teach, disclose or suggest conversion of the data format, which is different from encrypting data.

Saito and Scott, however, do not teach, disclose or suggest Applicant's: claim 37 limitations of

> said processing means controls said drive means to unlock the door on the basis of matching between the stored information in said storage means and the fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, wherein the fingerprint authentication token is independent of the main body and physically separated from the main body,

nor Applicant's claim 44 limitations of

> processing the first step comprises a second step of unlocking the door on the basis of matching between the stored information in the storage means and a fingerprint image from a fingerprint authentication token having the sensor for detecting the fingerprint image of the user as the biometrical information, wherein the token is independent of the main body and physically separated from the main body.

Since neither Saito, Scott, and therefore, nor the combination of the two do not teach, disclose or suggest all the limitations of Applicant's claims 37 and 44, Applicant's claims 37 and 44 are not obvious over Saito in view of Scott in view of Saito since a *prima facie* case of obviousness has not been met under MPEP §2142. Additionally, the claims that directly or

indirectly depend from claims 37 and 44, namely claims 42, and 49, respectively, would also not be obvious over Saito in view of Scott in view of Saito for the same reason.

Accordingly, withdrawal of the 35 U.S.C. § 103(a) rejection for claims 42 and 49 is respectfully requested.

CONCLUSION

In view of the foregoing, it is submitted that claims 1-2 and 4-93 patentably define the subject invention over the cited references of record, and are in condition for allowance and such action is earnestly solicited at the earliest possible date. If the Examiner believes a telephone conference would be useful in moving the case forward, he is encouraged to contact the undersigned at (310) 207-3800.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§1.16 or 1.17, particularly, extension of time fees.
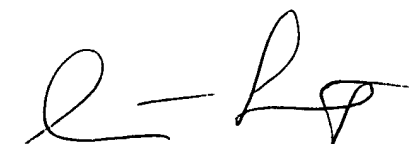
PETITION FOR EXTENSION OF TIME

Per 37 C.F.R. 1.136(a) and in connection with the Office Action mailed on March 9, 2006, Applicant respectfully petitions the Commissioner for a two (2) month extension of time, extending the period for response to August 9, 2006. The Commissioner is hereby authorized to charge payment to Deposit Account No. 02-2666 in the amount of $450.00 to cover the petition filing fee for a 37 C.F.R. 1.17(a)(2) large entity. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

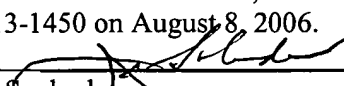BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN

Dated: August 8, 2006

Steven Laut, Reg. No. 47,736

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail with sufficient postage in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P. O. Box 1450, Alexandria, Virginia 22313-1450 on August 8, 2006.

Jean Svoboda